UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,702	03/22/2004	Steven J. Winick	H0006502-0555 (17268)	8726

128 7590 07/15/2009

HONEYWELL INTERNATIONAL INC.
PATENT SERVICES
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
07/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,702	WINICK, STEVEN J.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-13,15-18,20,28-32,34-36 and 38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-13,15-18,20,28-32,34-36 and 38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 20 April 2009 has been entered.

2. Claims 1-7, 9-13, 15-18, 20, 28-32, 34-36 and 38 have been presented for examination.

3. Claims 8, 14, 19, 21-27, 33, and 37 have been cancelled as per applicant's amendment.

Response to Arguments

4. Applicant's arguments filed 20 April 2009 have been fully considered but they are not persuasive.

5. In response to applicant's argument that the prior art does not show a system that uses a first security system to detect theft of an electronic device and a second security system for detecting use of the electronic device in an unauthorized network, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

6. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as a first security system to detect theft of an electronic device and a second security system for detecting use of the electronic device in an unauthorized network, are not recited in the rejected claims.

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, Suters is directed to a security system that detects the theft of an electronic device as seen by the title of the application, in addition to paragraph 0001 of the specification. Additionally, column 15, lines 1-40 discuss checking to make sure a device is in an authorized location, wherein that loaction may be a network.

7. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

8. See further rejections set forth below.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-7, 9-13, 15-18, 20, 28-32, 34-36, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2007/0118645 A1 to Suters, hereinafter Suters, in view of U.S. Patent No. 7,295,556 B2 to Roese et al., hereinafter Roese.

11. As per claims 1, 10 and 28, Suters discloses an electronic device in a local area network, comprising:

a network interface that communicates with a connection point of the local area network, and that receives a polling signal from a security system in the local area network via the

connection point (paragraph 0008, i.e. network manager device polls devices to see if they reply); and

a control that causes the network interface to communicate a response to the security system via the connection point in response to receipt of the polling signal (Figure 4 [block 401], paragraph 0039, i.e. receiving the state of a CE device), said control generates an alarm if said electronic device is not present (Figure 4 [blocks 402, 405], paragraph 0039, i.e. if the reception times out, meaning no response has been received, generating an alarm).

12. Suters does not teach a control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device, wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier and wherein said user interface is configured to allow a user to arm and disarm building intrusion detection features separately from security features of said LAN.

13. Roese teaches a control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device through the Internet (Figures 5 [step 505], 7 [steps 710, 715], column 18, lines 4-15, column 25, lines 33-58, column 31, lines 31-48, i.e. transmitting location information that may be encrypted with a key);

wherein said message includes an address and an identifier associated with the electronic device (column 36, lines 21-30, i.e. device specific information includes an IP address and a serial number) and said second security system verifies that said electronic device is installed in

an authorized network based upon said address and said identifier (Figures 5 [steps 510, 520], 6 [steps 620, 620b, 620a], column 25, lines 41-58, column 27, line 52 to column 28, line 3).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device, wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier, since Roese states at column 6, line 56 to column 7, line 7 that providing such features allows for the tracking of stolen devices which allows recovery or at the very least disabling access to sensitive information.

15. Suters and Roese does not disclose a user interface is configured to allow a user to arm and disarm building intrusion detection features separately from security features of said LAN.

16. It would have been obvious to one of ordinary skill in the art to provide an interface that arms/disarms a building intrusion detection system separately from the security features of a LAN, since one of ordinary skill in the art would clearly recognize that the building security features are a separate system from the network security features thereby requiring two separate interfaces for each system.

17. Examiner's NOTE: U.S. 2007/0118645 A1 qualifies as a 102(e) reference since it claims the benefit of an international application (WO/2005/048088). The International Application has met the following criteria to qualify the international filing date as the U.S. filing date: 1) the international filing date was after 29 November 2009 (11 November 2004); 2) it designated the

United States; and 3) it was published under PCT Article 21(2) in English. Since the International Application properly claimed the benefit of an earlier filed U.S. provisional application, the Examiner is permitted to use the provisional application as the earliest possible filing date. See MPEP § 706.02(f)(1)(I)(C).

18. Regarding claims 2 and 11, Suters teaches the network interface communicates with at least one other electronic device in the local area network via the connection point to transfer entertainment content (paragraph 0024, i.e. the electronic devices communicating and inspecting each other).

19. Regarding claim 3, Suters discloses the network interface communicates, via the connection point, with a remote server that provides services for the electronic device (paragraphs 0024, 0030, 0031).

20. With regards to claim 4, Roese discloses the services include at least one of downloading software to the electronic device, performing remote programming of the electronic device (column 6, lines 11-23, i.e. system **100** can provision and configure devices), and uploading diagnostic data from the electronic device.

21. Regarding claims 5 and 16, Roese teaches discloses the connection point comprises at least one of a hub and a gateway (Figure 1 [element 114], column 31, lines 9-30).

22. Regarding claims 6 and 17, Roese discloses the network interface receives software from the security system via the connection point for configuring the electronic device as a sensor of the security system (column 6, lines 11-23, i.e. system **100** can provision and configure devices).

23. Regarding claim 7, Suters discloses the security system sets an alarm if it does not receive the response from the network interface after sending the polling signal to the network interface (paragraph 0008, 0039).

24. Regarding claim 9, Roese teaches the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique for a specified group of electronic devices (column 18, lines 4-15, column 25, lines 33-58).

25. Regarding claim 12, Roese discloses the network interface communicates, via the connection point, with a remote server that provides services for the security system (column 6, lines 11-23, i.e. system **100** can provision and configure devices).

26. With regards to claim 13, Suters teaches when the alarm is set, the network interface communicates a message to the remote server indicating that the alarm has been set (paragraph 0039, i.e. alarm-alert or the device is in a protected state).

27. Concerning claims 15 and 31, Roese teaches the message comprises at least a portion of an Internet Protocol address associated with the electronic device (column 36, lines 21-30, i.e. device specific information includes an IP address).

28. Regarding claim 18, Suters teaches means for monitoring at least one sensor for detecting intrusion in a building (paragraph 0011, i.e. an anti-theft system).

29. Regarding claim 20, Roese teaches the response to the polling signal is provided as an encrypted message using an encryption code that is unique for a specified group of electronic devices (Figures 5 [step 505], 7 [steps 710, 715], column 18, lines 4-15, column 25, lines 33-58, i.e. transmitting location information that may be encrypted with a key).

30. Regarding claim 29, Suters teaches the message is received from the electronic device (paragraphs 0008, 0039).

31. Regarding claim 30, Roese teaches the message is received from a server that provides services for the electronic device (Figure 4 [step 440], column 25, lines 3-31).

32. Regarding claim 32, Roese teaches the identifier comprises a serial number (column 36, lines 21-30, i.e. device specific information includes a serial number).

33. Regarding claim 34, Roese teaches the message is received as an encrypted message using an encryption code that is unique for a specified group of electronic devices (column 18, lines 4-15, column 25, lines 33-58).

34. Regarding claims 35, 36, and 38, Suters and Roese do not teach the said control is configured to not allow spoofing of said electronic device.

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made to not allow spoofing of an electronic device, since one of ordinary skill in the art that anti-spoofing techniques are well-known and commonly practiced in order to prevent unauthorized access to a network.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

37. The following patents are cited to further show the state of the art with respect to anti-theft systems, such as:

United States Patent Application Publication No. 2002/0108058 A1 to Iwamura, which is cited to show polling computers to determine whether they have been stolen.

United States Patent No. 5,406,260 to Cummings et al., which is cited to show detecting the removal of electronic equipment.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

40. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf